тируют внимание на использовании психологических аспектов человеческого поведения, то есть манипулировании человеческими слабостями и доверием. Они стремятся обмануть, убедить или ввести в заблуждение жертву, чтобы получить доступ к ее конфиденциальной информации такими методами.

Фишинг – рассылка обманных сообщений, маскирующихся под надежные источники, часто от имени руководства компании или службы безопасности банка. Вишинг – получение ценной информации и побуждение жертвы к определенным действиям по телефону. Захват аккаунтов электронной почты, мессенджеров и социальных сетей с последующей рассылкой сообщений от имени владельца. Часто это просьбы о финансовой помощи или ссылки на вредоносные программы. Спуфинг – создание и продвижение поддельных сайтов, имитирующих известные интернет-магазины.

Киберпреступления, несомненно, являются одним из наиболее распространенных способов проявления преступных действий в интернет-среде. Предупреждение кибервиктимного поведения в основном построено на информировании людей о различных способах мошенничества. Склонность к кибервиктимному поведению обусловлена наличием некоторых особенностей эмоционального характера и низкой осведомленностью о способах информационной преступности. Способность противостоять преступным действиям мошенников в Интернете должна базироваться на формировании у людей таких личностных особенностей, как самоконтроль эмоциональных реакций и поведения. Важна и тренировка высокой адаптации к быстро меняющейся информационной среде.

Едынак И.В.

Дальневосточный юридический институт МВД России имени И.Ф. Шилова (г. Хабаровск)

Искусственный интеллект в работе полиции: возможности и риски интеграции

Технологии искусственного интеллекта активно развиваются и внедряются абсолютно во всем в мире. На данный момент искусственный интеллект является одним из наиболее перспективных открытий в различных сферах деятельности человека. При этом в рамках применения некоторых из них, например в работе органов внутренних дел, существуют, помимо перспектив внедрения и дальнейшего развития использования, значимые риски. Применение традиционных методов борьбы с преступностью не позволяет нанести значительный ущерб результатам, чего нельзя сказать о современных технологиях. Если же безосновательно внедрять искусственный интеллект в работу полиции, то конфиденциальность используемых данных будет нахо-

диться под угрозой, правам человека может быть нанесен значительный урон. Все это указывает на актуальность рассматриваемой темы и необходимость разработки практических рекомендаций.

На данный момент искусственный интеллект интегрируется в работу полиции по разным направлениям. Одно из наиболее популярных направлений – автоматизация процессов. Искусственный интеллект в настоящее время способен:

1) в автоматическом режиме принимать заявления граждан, это уменьшает нагрузку на сотрудников и позволяет им более оперативно реагировать на вызовы;

2) генерировать отчеты, направляя в краткой форме все нужные сведения. Можно ставить задачу искусственному интеллекту по формированию различных документов, что также позволяет правоохранительным органам сокращать во времени различные процессы;

3) анализировать тексты, данная функция позволяет правоохранительным органам оперативно получать ключевые сведения из документа любого объема, что также ускоряет процесс получения различных доказательств и аргументов.

Если первое направление оказывает лишь небольшое влияние на эффективность деятельности правоохранительных органов, то следующие напрямую увеличивают ее – в первую очередь речь идет об анализе данных. В этой области также широка возможность использования искусственного интеллекта. Так, как в нашей стране, так и за рубежом технология применяется для автоматизированного сбора и анализа сведений с камер видеонаблюдений уже относительно давно. Во многих случаях это позволяет оперативно обнаружить подозреваемого или преступника. Сам человек редко способен с такой точностью и скоростью анализировать столь крупное количество информационных данных, следовательно, даже при наличии обширной сети видеонаблюдения лицо может скрыться от преследования. При оперативном выявлении необходимого лица вероятность успешного задержания значительно увеличивается. Дорожно-патрульная служба также применяет указанную технологию при выполнении своих функциональных обязанностей: в частности, в этом случае, искусственный интеллект определяет не лица, а номера автомобилей, их цвет и возможные повреждения на автомобиле. В результате значительно увеличивается вероятность обнаружения угнанных транспортных средств, а также развивается система поиска преступников путем отслеживания их перемещений по территории страны.

В иных ситуациях такая функция требуется для поиска пропавших без вести лиц. Связав в единую сеть камеры видеонаблюдения во всех населенных пунктах страны, возможно значительно увеличить вероятность идентификации как разыскиваемых правонарушителей, так и пропавших без вести

граждан. Таким образом, через это направление можно значительно повысить уровень деятельности правоохранительных органов.

Здесь же можно выделить следующее направление применения – анализ сведений с камер видеонаблюдения, данное направление позволяет искусственному интеллекту определить предположительно нестандартное поведение лиц с направлением необходимой информации соответствующим подразделениям правоохранительных органов. Оперативное выявление определенного события, происшествия, правонарушения значительно повышает как скорость реагирования сотрудников, так и эффективность поддержания правопорядка.

Высока роль искусственного интеллекта при анализе трафика в сети Интернет. Ряд систем позволяют обнаруживать угрозы в киберпространстве и своевременно уведомлять правоохранительные органы для принятия необходимых мер. Здесь же можно указать, что искусственный интеллект способен определять неординарные действия пользователей сети, что ведет к автоматизированной блокировке операций, следовательно, предотвращаются, например, преступления в сфере мошенничества. В рамках кибербезопасности можно выделить блокировку опасного контента, размещенного на сайтах. Искусственный интеллект производит ее самостоятельно, следовательно, информация, находящаяся в открытом доступе, наносит минимальный ущерб обществу. Как итог, искусственный интеллект может значительно улучшить процесс противодействия киберпреступникам.

Предоставляя программе с искусственным интеллектом достаточное количество информации, можно получить значимые оценочные сведения. Так, искусственный интеллект может выявить районы повышенного криминального характера. Искусственный интеллект может рассчитать характер правонарушений для предоставления рекомендаций по предотвращению преступных действий на конкретной территории. Подобная работа может проводиться по всем населенным пунктам. Благодаря грамотному совмещению направлений работы, сотрудники правоохранительных органов получают оптимальные рекомендации по патрулированию улиц, что позволяет снизить уровень преступности, а также оперативно реагировать на возможные правонарушения. Технологии искусственного интеллекта могут обрабатывать и анализировать большие объемы информации из различных источников, включая отчеты о преступлениях, камеры наблюдения, социальные сети и публикационную активность. Это позволяет правоохранительным органам обнаруживать закономерности, а также определять направления, которые могут помочь в расследовании преступлений, обладать актуальной информацией о возможных угрозах и быстро на них реагировать.

Обобщая возможности применения, можно сказать, что искусственный интеллект способен уменьшить количество однотипных операций, возложенных на сотрудников полиции, увеличить вероятность обнаружения право-

нарушителей, предупредить о проблемах с соблюдением общественного порядка, предсказать наиболее неблагополучные территории и так далее. В результате деятельность правоохранительных органов становится более эффективной.

Несмотря на многочисленные преимущества, интеграция искусственного интеллекта в работу полиции может создать ряд рисков.

Первым и наиболее значимым является перспектива нарушения конфиденциальности.

Нельзя не отметить проблемы профилирования: искусственный интеллект в случае его неудачного обучения или наличия индивидуального мнения у создателя способен демонстрировать ложную связь между различными элементами.

Исходя из рассмотренных в рамках данного материала направлений развития применения искусственного интеллекта можно предложить следующее:

1) проведение мероприятий по расширению применения искусственного интеллекта в органах внутренних дел с учетом специфики деятельности подразделений;

2) допуск к разработке и обучению программ с искусственным интеллектом только высококвалифицированных специалистов;

3) проведение обязательного тестирования разработанных и обученных систем перед их широким применением на практике;

4) проработка возможности разработки программ дополнительного профессионального обучения лиц, способных эффективно использовать программное обеспечение с искусственным интеллектом.

Кошкина В.В.

Владивостокский филиал
Дальневосточного юридического института МВД России им. И.Ф. Шилова

Криминологические меры противодействия преступлениям, совершаемым с использованием компьютерных и телекоммуникационных технологий

Качественное и своевременное реагирование государства на изменение структуры и характера преступности является первостепенной задачей для обеспечения прав и свобод человека и гражданина. В современной действительности, где технологические возможности с каждым днем развиваются и становятся более сложными, необходимо принимать все необходимые меры для противодействия преступности, особенно с использованием информационных технологий.